Strategy Research Project

CYBERSPACE OPERATIONS: INFLUENCE UPON EVOLVING WAR THEORY

BY

COLONEL KRISTIN BAKER
United States Army

DISTRIBUTION STATEMENT A:
Approved for Public Release.
Distribution is Unlimited.

USAWC CLASS OF 2011

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College, Carlisle Barracks, PA 17013-5050

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)* 18-03-2011	**2. REPORT TYPE** Strategy Research Project	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE

Cyberspace Operations: Influence Upon Evolving War Theory

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Colonel Kristin Baker

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Professor Jeffrey Caton (Colonel, USAF, Retired)
Center for Strategic Leadership

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Cyberspace has reshaped the strategic environment in which the world's players conduct activities requiring senior military leaders to develop a new theory of war incorporating this dynamic and complex battlespace. As the world's oceans have provided a means to conduct commerce and wield power throughout history, cyberspace today provides the same to powerful nations with conquering militaries. The significant difference today is that cyberspace provides those opportunities not only to powerful nations, but also to lone actors whose individual actions can have strategic affect given the speed with which communications and actions are transmitted on the digital infrastructure. The U.S. needs a strong defense in cyberspace against those who wish it harm, as well as a strong offense supported by international laws governing the use of cyberspace operations. This paper addresses both the opportunities and challenges posed in this new dimension as well as the implications of operating in cyberspace for the U.S. The U.S. must take a leading role in developing laws governing cyberspace operations both as a battlespace and as a place of commerce and communications.

15. SUBJECT TERMS

Cyber Power, Cyber Theory

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UNCLASSIFED	**b. ABSTRACT** UNCLASSIFED	**c. THIS PAGE** UNCLASSIFED	UNLIMITED	30	**19b. TELEPHONE NUMBER** *(include area code)*

USAWC STRATEGY RESEARCH PROJECT

CYBERSPACE OPERATIONS: INFLUENCE UPON EVOLVING WAR THEORY

by

Colonel Kristin Baker
United States Army

Professor Jeffrey Caton
Project Advisor

This paper is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Colonel Kristin Baker

TITLE: Cyberspace Operations: Influence Upon Evolving War Theory

FORMAT: Strategy Research Project

DATE: 18 March 2011 WORD COUNT: 5,656 PAGES: 30

KEY TERMS: Cyberpower, Cyber Theory

CLASSIFICATION: Unclassified

Cyberspace has reshaped the strategic environment in which the world's players conduct activities requiring senior military leaders to develop a new theory of war incorporating this dynamic and complex battlespace. As the world's oceans have provided a means to conduct commerce and wield power throughout history, cyberspace today provides the same to powerful nations with conquering militaries. The significant difference today is that cyberspace provides those opportunities not only to powerful nations, but also to lone actors whose individual actions can have strategic affect given the speed with which communications and actions are transmitted on the digital infrastructure. The U.S. needs a strong defense in cyberspace against those who wish it harm, as well as a strong offense supported by international laws governing the use of cyberspace operations. This paper addresses both the opportunities and challenges posed in this new dimension as well as the implications of operating in cyberspace for the U.S. The U.S. must take a leading role in developing laws governing cyberspace operations both as a battlespace and as a place of commerce and communications.

CYBERSPACE OPERATIONS: INFLUENCE UPON EVOLVING WAR THEORY

> We meet today at a transformational moment -- a moment in history when our interconnected world presents us, at once, with great promise but also great peril.[1]
>
> —President Barack Obama
> Securing Our Nation's Cyber Infrastructure

The 21st Century has thus far exhibited a propensity to be defined by near constant conflict waged not only on battlefields from Iraq to Afghanistan and on the world's oceans but in the media, through the Internet, and across the global digital infrastructure. American military leaders need an expanded theory of war that includes this new dimension of battle—cyberspace. This paper will address the concept of cyberspace and the activities currently occurring in it. It will further describe the ways in which the development of cyberspace is shaping the strategic environment while exploring the writings of military theorists from Sun Tzu to Gulio Douhet in an effort to develop an updated theory of warfare for the 21st Century.

Though the nature of warfare itself has not changed, —conflict is still waged between people over resources, land, pride, and power—the development of the Internet, the incredible access to information it provides, and the speed of communications and commerce facilitated by the digital infrastructure in cyberspace have irreversibly expanded the environment in which warfare and conflict are waged. The impact of this change in the way world powers, economic entities, and private citizens interact and function cannot be underestimated. As President Obama noted in the epigraph, this new form of interaction is both a blessing, in that it offers incredible flexibility in global communications and commerce, and a curse in that it is extremely vulnerable to exploitation by criminals, foreign adversaries, and adversarial non-state actors who might wish the U.S. and its citizens harm. Understanding cyberspace and adapting war theory to account for cyberspace is an integral component of ensuring the continued success of the U.S. in the 21st Century.

International Modern World Order: Understanding the Cyberspace Global Commons

In order to develop an adapted theory of war that embraces cyberspace as a new battlespace, it is first important to have a common understanding of what cyberspace is. There is much debate today both in the U.S. and within the international community on whether cyberspace is a domain, a group of computers or devices on networks that are administered under the same protocol,[2] or a tool, something that can be used to facilitate activity. The answer is that it is both. Cyberspace is a domain that facilitates the movement of goods, communications, and services. Within cyberspace there exist tools that allow criminals to steal intellectual property, money, and goods; adversaries to commit espionage; and non-state actors to communicate their messages globally. The DoD defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[3]

Another phrase frequently used to define cyberspace is "global commons." The current legal definition of "global commons" is "geographical areas that are outside the jurisdiction of any nation . . .."[4] Based on this definition, it is evident why the application of the term "global commons" when discussing cyberspace is compelling. As the world's oceans have historically been considered a global commons that facilitate the transit of commerce and communications, cyberspace provides that same function today. The concept of cyberspace as a global commons has gained traction as evidenced by the North Atlantic Treaty Organization's inclusion cyberspace as part of its Global Commons Initiative. In this initiative, NATO notes the global commons are "the connective tissue of international security . . . comprised of maritime, space, and cyber components."[5]

Another key aspect to understanding cyberspace is in appreciating how cyberspace serves not only to facilitate commerce and communications but as battlespace for the conduct of warfare. Chinese war theorist Sun Tzu noted over 2,000 years ago "In respect to employment of troops, ground may be classified as dispersive, frontier, communicating, focal, serious, difficult, encircled, and death."[6] In the 21st Century, cyberspace and the global community operating in it represent communications ground; terrain that may prove to be the most difficult on which the U.S. must operate. Building on Sun Tzu's communications terrain concept and borrowing from Julian Corbett's seapower theory, it is useful to consider that cyberspace is to cyber war what the oceans are to war at sea. As the oceans provide "a means of communication for national life" as well as an opportunity to affect an enemy through "commerce prevention"[7] so cyberspace offers a line of communication for national life and an opportunity to deny the enemy logistic support, funding, and a means of communicating military information. If battles are fought as a means to "exert pressure on the citizens and their collective life,"[8] the fact that people across the globe are now on the cyberspace battlefield provides a unique opportunity to achieve this objective rapidly . Alfred Thayer Mahan, also a seapower theorist, made the connection between the oceans and global commons when he stated "The first and most obvious light in which the sea presents itself from the political and social point of view is that of a great highway; or better, perhaps of a wide common over which men may pass in all directions . . ..”[9] As people may pass in all directions on the sea, so may they virtually transit the global digital infrastructure through cyberspace in all directions.

Though travel across the globe through the ocean could theoretically take any water path, the locations of ports and chokepoints channel sea routes just as the locations of ground-based service providers and communications nodes tend to channel digital traffic. In 2007, researchers at Bar Ilan University in Israel conducted a compelling study of the Internet that considered not only how it is connected but also how it functions. They discovered that the Internet has at its core approximately 80 critical nodes. Another 15,000 peer-connected, or self-sufficient, nodes surround this core. Outside of the dense core and the peer layer, there are another 5,000 isolated nodes that are loosely connected.[10]

Having noted the similarities between the ocean as a domain and cyberspace, it is important to note that the two differ in two important ways. First, the global digital infrastructure is vast, complex, and constantly evolving. Maps showing the topology of the Internet look more like images of the neural networks across the human brain than maps of sea routes. Whereas sea routes remain relatively consistent, both cyber and neural networks are constantly changing; neural networks are created and broken routinely in the brain as information transits the body just as connections within the digital infrastructure are established and broken near constantly as information attempts to transit the most efficient route available at a given time. Secondly, operators on both the seas and the cyberspace rely on ports to begin and complete their journeys. Without seaports the oceans continue to exist. Without cyberspace ports,[11] there is no cyberspace. It is in understanding the key cyberspace ports, or critical nodes, and the opportunities they present that the U.S. can begin to build both offensive and defensive plans to operate on the global digital infrastructure.

Given a common understanding of what cyberspace is, developing a theory of war that includes cyberspace operations requires an understanding of how cyberspace has shaped the strategic environment. The strategic environment of the 21st Century and the significance of cyberspace can be defined by three key characteristics. First, it is a unipolar world with the U.S. at the helm unmatched in traditional military power; this unipolar environment has led to a situation in which potential and real enemies believe the U.S. can only be defeated by asymmetric, or indirect, attack. Second, it is a globalized world in which information on conflict is broadcast twenty-four hours a day into the homes of its people, making war a part of their lives and the people part of every war. Third, it is an interconnected world in which the security of trade, communications, and freedom of speech relies on the security of a network designed to make information accessible not defensible, exposing perhaps the most dangerous global vulnerability to the effects of an enemy savvy in the conduct of hostile cyberspace operations.[12]

The World Today: Warfare in an Asymmetric Century

Given the likelihood that the U.S. will remain unmatched in military power in the foreseeable future, this Century will continue to be defined by enemies searching for and finding new and old asymmetric ways—the short ways--to attack the U.S. and its interests. Sun Tzu recognized the complex nature of war in a unipolar world when he noted “He who wishes to snatch an advantage takes a devious and distant route and makes of it the short way.”[13] With these words, Sun Tzu describes the complex environment the U.S. faces today made up of rising powers such as the People’s Republic of China (PRC), Russia, and India, insurgent forces such as those the U.S. is actively fighting in Iraq and Afghanistan, as well as terrorists with global agendas, such as al-Qa’ida all who wield asymmetric power in cyberspace. Nation states leverage accesses built in cyberspace to steal their adversaries’ state secrets. Terrorist groups use cyberspace not only as a platform for recruiting future members but also as a venue to raise funds for their activities and as a vehicle for planning terrorist attacks.[14]

David Rapoport, in his work “The Four Waves of Modern Terrorism,” provides evidence of how the environments in which terrorist groups operate shapes the groups and tools of warfare they choose. He describes four different “waves” of terrorism and the varying tools used in each to conduct warfare. Each wave is shaped by the world in which it existed and can only be understood in context of the strategic environment of the time. Whereas bank robberies provided a source of income to fund activity of the anarchists, the anti-colonial freedom fighters were successful in obtaining funds from dispersed Diaspora communities. Anarchists used assassinations to kill public officials while the “New Left” conducted assassinations as a form of punishment and used kidnapping to obtain funds.[15] Today’s wave of insurgents has similarly adapted, using cyberspace to proliferate their message.

It is important to note that cyberspace, though a battlespace in the broader war waged by terrorists and/or extremists, is neutral ground, not owned or occupied by either side. Just as a terrorist group can use the Internet to spread its anti-government message, governments can and must use the Internet to boost their own legitimacy. Here we can take valuable advice from Sun Tzu when he asserted, “what is of supreme importance in war is to attack the enemy’s strategy.”[16] If the adversary’s strategy relies on gaining popular support and creating conditions in which it can fight an extended war on the ground and in cyberspace, the U.S. and its allies return fire by denying the enemy that popular support. Countering the enemy’s strategy early denies him the opportunity to create a situation in which the insurgency has no apparent end.

Cyberspace offers the U.S. two ways in which to counter threat actors. First it proffers the same battlespace in which to counter extremist messages. Second, it provides an opportunity to “attack” an enemy using what would typically be considered a traditional nation state tool: “commerce prevention”[17] or blockade. As evidenced by the recent actions taken by PayPal, Visa, and MasterCard to deny use of their web services to facilitate donations to the organization, WikiLeaks, following a large leak of sensitive U.S. diplomatic communications,[18] cyberspace blockades are not only possible but already in use.

It is becoming increasingly clear that nation states such as Russia and the PRC understand the value of conducting asymmetric activity in cyberspace. Though Russian complicity is unproven in the 2007 cyberattack in Estonia that resulted in the freezing of bankcards and mobile phone networks, the attacks came at a time of increased tensions between Russia and Estonia leading many analysts to assess that Russia was behind the attacks.[19] The PRC’s interest in using cyberspace to support asymmetric activity can be traced back as far as 1999 when Chinese Army Colonels Qiao Liang and Wang Xiangsui published a book entitled *Unrestricted Warfare*. In their book they advocated a strategy of warfare that included hacking into websites, targeting financial institutions, and using the media as asymmetric means to overcome the military superiority of the U.S.[20] Recent evidence of PRC's ongoing use of cyberspace to conduct digital network exploitation is extensive, though actual state sponsorship of the same activities is difficult to prove.

Cyberspace, War, and People

Cyberspace has reshaped the strategic environment by making the world and its conflicts accessible to its individual citizens through tools such as the Internet. Though both Clausewitz and Sun Tzu recognized wrote about the importance of the people in warfare, the unique challenge of managing the passions of the people given immediate access to conflict is more difficult than either theorist could have envisioned when they authored their seminal works.

> In a millisecond, satellite images depicting population migrations can be transferred from the office of Refugees International in Washington, D.C. to a remote computer in El Fashir Sudan . . . In the same time span, a disaffected Somali-American living in St. Paul, Minnesota can send remittances to Mogadishu, Somali to support the cause of Al Shahab insurgents. [21]

It is this aspect of the strategic environment that most uniquely characterizes the 21st Century. Today, individuals with no military experience are more aware of war and can participate in war-related activities from the comfort of a home office.[22] The people are involved in warfare and the battlefield, expanded to include cyberspace, is flooded with civilians.

Not only are average citizens more involved through use of the Internet and social media, but the Soldiers who fight the nations' wars are more accessible to non-combatants through the same. The U.S. military has grappled with how to handle the challenges associated with civilians in cyberspace and with its own soldiers sharing the war through daily blogs. Though controversial at the time, in early 2008 Lieutenant General William Caldwell, Commanding General of the Combined Arms Center, acknowledged both the significance of the Internet to U.S. adversaries but also the opportunity the Internet provided to allow soldiers to share their personal stories on-line with an American audience hungry for insight into the lives of military personnel in the war. He wrote in a blog on Small Wars Journal " . . . we must encourage our Soldiers to interact with the media, to get onto blogs and send their YouTube videos to their friends and family. When our Soldiers share/tell their stories, it has an overwhelmingly positive effect."[23]

The People's Republic of China, too, appears to have grasped this new aspect of warfare as evidenced by their employment of "patriotic hackers" in the conduct of Internet activity. According to China cyber expert and a director at the Center for Intelligence Research and Analysis, James Mulvenon, the PRC has a different approach to the execution of cyber warfare that leverages Chinese citizens to volunteer internet hacking skills to support PRC national objectives.[24] Many analysts have pointed out that this practice of using citizens to support broader national objectives is reflective of Mao Tse-tung's concept of mobilizing "the whole people to unite as one man and carry on the war with unflinching perseverance."[25]

In order to ensure support of both its people and its allies, the U.S. must retain the moral high ground and avoid the misuse of its national power in cyberspace that could result in increased repression of the same people the U.S. intends to positively influence.[26] Sun Tzu stated, "Those skilled in war cultivate the Tao and preserve the laws and are therefore able to formulate victorious policies."[27] Our current National Security Strategy reflects this principle noting "Our values have allowed us to draw the best and brightest to our shores, to inspire those who share our cause abroad, and to give us the credibility to stand up to tyranny."[28] The U.S. must take a leadership role in both increasing regulation to limit illicit activity in cyberspace and in using cyberspace to continue to spread its message of democracy and freedom to all people.

Defensive Operations in Cyberspace

If access to cyberspace uniquely characterizes the current strategic environment, defending that access may present the greatest military and governmental challenge in the 21st Century. President Barack Obama made it clear that securing America's cyber infrastructure is a national security priority by officially declaring the U.S. digital infrastructure as a "strategic national asset" in the May 2010 National Security Strategy.[29] The Internet, designed to provide rapid exchange of vast amounts of information, was not built for the protection of that information. The lack of network defenses has not been lost on those entities that wish to do U.S. harm and building those defenses has proven to be difficult for nations, citizens, and corporations alike.

Telling is the testimony Mr. Larry Wortzel, Commissioner of the U.S.-China Economic and Security Review Commission, provided to the Committee on Foreign Affairs in the House of Representatives on March 10, 2010. Mr. Wortzel stated "foreign intelligence or military services penetrate the computers that control our vital national infrastructure or our military, reconnoiter them electronically and map or target nodes in the systems for future penetration or attack."[30] According to one study on the Chinese People's Liberation Army and their intended use of information warfare (IW), "one of the most interesting Chinese IW concepts is the notion of overcoming the superior with the inferior" [31] by engaging the U.S. using IW.[32] The same study further notes "many Chinese writings suggest that IW will permit China to fight and win an information campaign, *precluding the need for military action"* (emphasis in original).[33]

Currently, providing security of the cyber infrastructure is conducted in a disjointed or perhaps even haphazard fashion. The Department of Homeland Security's (DHS) Office of Cybersecurity and Communications is responsible for the security of the federal government's cyber infrastructure as well as for providing a bridge between the federal government and the private sector through its U.S. Computer Emergency Readiness Teams (USCERT).[34] The Department is also charged with coordinating the critical infrastructure protection activities of private companies.[35] The newly operational U.S. Cyber Command (USCYBERCOM) provides oversight of the security of DoD networks. [36] In an effort to improve synchronization of the roles of the DoD and the DHS, the two agencies signed a memorandum of agreement on 10 October 2010 designed to "increase interdepartmental collaboration in strategic planning for the Nation's Cyber security, mutual support for cyber security capabilities development, and synchronization of current operational cyber security mission activities."[37] In the private sector, individual corporations are responsible for providing security for their corporate networks and private citizens provide the same for their personal computers and home networks.

This dispersed approach to providing cybersecurity to the nation's digital infrastructure is proving to be inadequate. The cybersecurity company Symantec reported in August 2010 that 1 in 74.6 emails addressed to government/public was blocked as malicious, making this sector the most targeted industry for malware.[38] The company Mobile Active Defense Partners, LLC estimates that there are more than 100 million computers currently part of criminal networks,[39] many of which are likely personally-owned computers that have been pulled into botnets[40] through viruses unbeknownst to their owners. According to a recent study by cybersecurity provider McAfee, over one trillion dollars was lost to cybercrime last year both in the form of intellectual property and the costs associated with addressing cyber intrusions.[41] Given statistics like these as a backdrop, it is clear why the U.S. is concerned about its national cyber infrastructure. It is also clear that malicious threats to this infrastructure are not only directed at the federal government, but at corporations, the DoD, and private citizens. Over the last few years, there has been increasing deliberation both in the government and private sector regarding the government's role in regulating the nation's cyber infrastructure.

There are several key concerns regarding the government's involvement in protecting the digital infrastructure. First is the concern that government oversight will result in either a violation of citizens' privacy or a reduction in civil liberties. Cyber blogger and author Jim Harper argues that the U.S. government should not be responsible for providing computer security to private citizens any more so than the government is responsible for securing an individual's home.[42] The flaw in this analogy is that a neighbor's careless home security practices do not result in letting a burglar into another neighbor's living room. Due to its interconnectivity, careless security practices on one part of the network quickly result in intrusions on another; the federal government, corporate America, and the average citizen all share the same digital network.

Those who argue against more government involvement in providing private and public sector cybersecurity are concerned that their privacy may be compromised by government oversight; ironically it is the same privacy the government would like to protect that is being violated by criminal internet activity such as identity theft. Large corporations, however, are beginning to recognize the need for more government involvement in protecting against the loss of intellectual property and money due to cyber crime. In one recent study, Mr. David Batz of the Edison Electric Institute noted that because the government obtains classified actionable intelligence regarding cyber threat activity, there must be closer coordination between government and private/public sector entities.[43]

Another concern regarding governmental involvement in providing national cybersecurity is the lack of international laws or norms in cyberspace. As retired Director of National Intelligence Admiral Dennis C. Blair recently noted, "The precedents and the laws on the books are just hopelessly inadequate for the complexity of the global information network."[44] The U.S. government is leaning forward, however, in this effort. The Office of the Director of National Intelligence recently asked the National Research Council (NRC) to research strategies to deter cyberattacks. The NRC brought together experts in cybersecurity across the U.S. who researched and wrote papers on various issues to include a review of international law as it relates to cyberspace operations. These papers provide a good framework for the execution of cyberspace operations and should be carefully studied as the federal government goes forward.[45]

There are two methods for providing defense to the digital infrastructure: passive defense and active defense. Passive defensive measures today provide security in much the same way walled cities and moats did centuries ago. Passive measures include applications such as firewalls, anti spyware, and antiviral software, designed to detect attempted intrusions into a user's system and block them. Passive defensive measures are generally minimally intrusive and do not affect any computer or network but those they are designed to protect, making them more broadly acceptable forms of defense. Unfortunately, cyber criminals, hackers, and even foreign governments are creating worms, viruses, and botnets faster than cybersecurity companies can develop and field countermeasures.

Active defensive measures are more effective, but also more controversial. Active defensive measures are roughly the equivalent of counterstrikes. For example, if an intrusion is detected on a network, active measures might allow the attack or intrusion to be tracked back to its origin and then engaged in some way that affects the attacker's computer system.[46] Aggressive active defensive measures could present a danger on the globally connected network for several reasons. First, it is difficult to control the path of a cyber counterstrike given that many attackers or criminals will use third party Internet service providers, potentially in third countries, to cover the trail their intrusion might leave behind. Second, and perhaps most importantly, international law is very unclear as to the legal restrictions of conducting such activity by individual persons or international companies and governments on the global network.

Though international law with regard to cyberspace operations is evolving, there is little contention regarding a nation's right to passively defend its networks. Article 51 of United Nations' Charter recognizes a nation's right to self-defense and there is general international acceptance of the provisions of the UN Charter. Where the international standards are less clear is how far a nation can go to actively defend its networks or respond to a cyber attack through pre-emptive attack against an enemy in cyberspace.[47] Unfortunately, as evidenced by the examples offered in this paper, disjointed defensive actions based primarily on passive defensive measures alone are falling short of providing the necessary defense of the nation's cyber infrastructure. Sun Tzu observed the difficulty inherent in defense when he cautioned ". . . when he prepares everywhere he will be weak everywhere." [48]

In order to successfully execute defense of the digital infrastructure, the U.S. must task the Department of Homeland Security and DoD to provide passive and active defense, both kinetic and non-kinetic, of the government's networks in partnership with the public and private sector testing the limits of current international law. As incidents occur, the Department of State must use these incidents to garner support for a comprehensive review of international law and the establishment of new international norms and standards for defensive actions in cyberspace. The U.S. government must work within the international community to identify critical cyberspace nodes at the core and map and track the health of those critical portions of the network as the digital infrastructure evolves. As editorial director of the Computer Security Institute, Richard Powers, offered in an interview with news program Frontline, just as the government regulates critical utilities like electricity and telecommunications, it is time to develop rules for cyberspace operations.[49]

Offensive Warfare in Cyberspace

It is useful to draw a parallel between air power and cyber power when considering offensive action in cyberspace. Air power theorist, Guilo Douhet, noted "there is no practical way to prevent the enemy from attacking . . . with his air force expect to destroy his air power before he has a chance to strike . . ..."[50] As it is difficult to strike enemy air forces once launched as air power theorist Douhet alludes to above, it is similarly difficult to counter a cyber attack in progress. Attacking an enemy's cyber capabilities before he has a chance to use them certainly would be in line with another Sun Tzu principle "Attack where he is unprepared; sally out when he does not expect you."[51]

Though both Sun Tzu and Clausewitz acknowledge a role for defensive action in war, for both theorists defensive actions are temporary actions taken until the military forces are once again capable of conducting offensive operations. Sun Tzu noted "Invincibility lies in the defence; the possibility of victory in the attack."[52] Clausewitz asserted that the defensive form of warfare was the strongest form, but he went on to clarify that defense "has a negative object" and "that it should be used only so long as weakness compels and be abandoned as soon as we are strong enough to pursue the positive object."[53] In its critical role of providing traditional land, air, and sea forces to protect the U.S.' homeland, the DoD does not lack clarity in its approach. Per Joint Publication 3-27 Homeland Defense, the U.S. military may take action to "destroy, degrade, disrupt, or neutralize" threat capabilities "before they are employed by an adversary.[54] It is time for the U.S. to adopt a similar strategy for the execution of war in cyberspace.

One needs look no further than the 2008 Russian attack on Georgia for evidence of the emerging role of cyber attack in the conduct of state-on-state conflict. During a period of high tension between Russia and Georgia over South Ossetia, and just prior to Russian ground forces moving in to the disputed territory, a massive denial of service attack was launched on Georgian web sites.[55] The cyber attack rendered the Georgian government nearly incapable as its file servers were crippled, Georgian web sites defaced, and Georgian banks overwhelmed by denial of service attacks. Though attributing the cyberattacks to the Russian government was not possible at the time, political analysts assess that the Russian government was likely complicit in the attacks based on the sophistication of the attacks.[56] The Georgian National Security Council Secretary, Eka Tkeshelashvili, referred to the cyber attacks as a Russian attack on a fourth front; the first three fronts being land, sea, and air.[57]

One of the primary reasons there is little legal clarity regarding acceptable responses to aggressive cyber intrusions or attacks is the limited ability to trace the source of the activity back to a specific actor in cyberspace. There remain valid concerns that direct cyberspace operations will either hit the wrong target or have unintended consequences elsewhere on the network. Of note, indisputable positive identification of the enemy has never been an absolute imperative in war. Though a moral actor would prefer to be able to identify every target as a specific valid, military target, the fog and friction of war often preclude such certainties. Counter-battery fire provides a good example of this principle. Artillery fire is exchanged between ground-based sites potentially hundreds of miles apart. Units on the ground respond by conducting counter-battery operations directed at an enemy they cannot see. Arguably a cyberattack’s path is far more difficult to identify than an artillery trajectory, but as nations work together to create a less lawless and more regulated cyberspace, uncertainty will decrease. It may take one round of fires and counter-fires to generate enough concern within the international community to focus efforts on increasing regulation of the Internet, but the U.S. must assume a leadership role in shaping future international cyberspace operations norms.

U.S. Cyber Command: A Step in the Right Direction

In order to effectively operate in cyberspace, the U.S. must create organizations responsible for executing its cyberspace operations. On 23 June 2009, Secretary of Defense Robert Gates signed a memorandum formally establishing USCYBERCOM.[58] Arguably one of the most contentious changes the DoD has undertaken in a decade, the establishment of the new command requires not just extensive planning and socialization, but a change in the culture of how the military thinks about and conducts cyberspace operations. No longer are cybersecurity and cyberspace operations the responsibility of disparate signal support units, intelligence community agencies, and separate service entities, but now cyberspace operations will be synchronized by a separate joint command led by a four star general. More than one year after Secretary Gates released his memorandum, USCYBERCOM is fully operational and the effort by strategic leaders to change DoD culture in regards to cyberspace operations and the roles and functions of USCYBERCOM continues.[59]

It is not only tackling the question “To secure or not to secure?” that makes USCYBERCOM’s challenge one of the toughest missions in DoD today but also “how much to secure and at what expense?” Every step the U.S. takes to secure its vulnerable networks also limits its ability to access information in the rapid, nearly unfettered means to which Americans have become accustomed. The U.S. military network today allows near- real-time access to information across the globe in support of operations ranging from logistics to intelligence. According to one report, the current military global communications network consists of "15,000 networks and seven million computing devices across hundreds of installations in dozens of countries."[60]

The development of USCYBERCOM and the increasing role the Department of Homeland Security (DHS) is playing in conducting cyberspace operations on behalf of the U.S. is proving to be timely. As demonstrated by the cyber attacks allegedly conducted by Russia as part of its kinetic attacks into Georgia in 2008 noted earlier in the paper[61] and the increasing evidence that China is conducting daily intrusions into U.S. military and corporate networks,[62] it is only a matter of time before USCYBERCOM and DHS leadership will have an opportunity to respond to a cyberspace crisis. Stuxnet, the malicious worm some experts believe was designed by a nation-state to sabotage Iran's nuclear program,[63] presages the likely near- future of cyberspace operations. Fortunately, Stuxnet, the "cyber shot heard around the world" as one reporter described it, was most likely aimed not at the U.S. but at Iran—this time.[64] What comes after Stuxnet and what that means to the cyberspace capabilities of the U.S. are the questions USCYBERCOM and DHS will need to address.

Conclusion: War for the 21st Century

As this paper demonstrates, the nature of war in the 21st Century may not change but the strategic environment in which nations fight has changed dramatically due to the expansion of operations in cyberspace. The U.S. can and should prepare for this new environment by assuming a leading role in shaping the international norms in cyberspace. War theorists from Sun Tzu to Corbett provide useful advice that is as appropriate today as it was when it was written for this expanded domain has more similarities to land, sea, and air space than dissimilarities.

The U.S. must prepare both passive and active defenses for its digital infrastructure while helping develop international law defining acceptable behavior by state and non-state actors in this ever-expanding cyberspace commons. The U.S. military must be prepared to conduct counter strikes in cyberspace in order to maintain its military advantage and protect the interests of the nation and its allies and partners. Leaders in both the Department of Homeland Security and the DoD are beginning to make strides toward defining cyberspace and their respective roles and missions in this complex, ever-changing environment. Lastly, but perhaps most importantly, the U.S. and the international community must accept that the incredible access to information and capabilities the global digital infrastructure provides are going to increase making average citizens more aware of and more a part of conflict than ever. People have always waged wars whether over resources or pride and it is in determining how to best harness this energy in cyberspace that the U.S. will maintain its role as a superpower into the 21st Century.

Endnotes

[1] President Barack Obama, "Remarks by the President on Securing Our Nation's Cyber Infrastructure," May 29, 2009, linked from The White House, http://www.whitehouse.gov/ the_press_office/ Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/ (accessed October 8, 2010).

[2] "Domain | Define Domain at Dictionary.com," *Dictionary.com*, http://dictionary.reference.com/browse/domain (accessed February 3, 2011).

[3] *Cyberspace Operations Concept Capability Plan 2016-2028*, February 22, 2010, http://www-tradoc.army.mil/tpubs/pams/tp525-7-8.pdf (accessed February 3, 2011).

[4]"Global Commons Law & Legal Definition," *Legal Definitions Legal Terms Dictionary*, http://definitions.uslegal.com/g/global-commons/ (accessed December 8, 2010).

[5]"The Global Commons," linked from the *North Atlantic Treaty Organization Allied Command Transformation*, http://www.act.nato.int/globalcommons (accessed December 8, 2010).

[6]Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press. Inc., 1963), 130.

[7]Julian Corbett, "Theory of the Object--Command of the Sea," in *U.S. Army War College Guide to National Security Issues Vol. I: Theory of War and Strategy*, (Carlisle Barracks, PA: U.S. Army War College, 2010), 206-207.

[8]Ibid., 208.

[9]Alfred Thayer Mahan, *The Influence of Sea Power Upon History, 1660-1783* (Little, Brown, and Co., 1891), Google e-book.

[10]Duncan Graham-Rowe, "Mapping the Internet - Technology Review," *Technology Review: The Authority on the Future of Technology,* http://www.technologyreview.com/infotech/18944/?a=f (accessed December 4, 2010).

[11]Cyberspace ports are those points of contact on the ground where digital messages are moved to individual users; typically network servers.

[12]Cyberspace operations is defined as the employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid. DoD Dictionary of Military and Associated Terms, Joint Publication 1-02, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (accessed February 03, 2011).

[13]Sun Tzu, *The Art of War*, 102.

[14]Eben Kaplan, "Terrorists and the Internet - Council on Foreign Relations," *Council on Foreign Relations*, http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005#p2 (accessed February 3, 2011).

[15]David Rapoport, "The Four Waves of Terrorism," in *U.S. Army War College Guide to National Security Issues Vol. II: Theory of War and Strategy,* (Carlisle Barracks, PA: U.S. Army War College, 2010), 227-249.

[16]Sun Tzu, *The Art of War*, 77.

[17]Corbett, *U.S. Army War College Guide to National Security Issues Vol. I: Theory of War and Strategy,* 207.

[18]Mark Townsend, Paul Harris, Alex Duval Smith, Dan Sabbagh, and Josh Halliday, "WikiLeaks backlash: The first global cyber war has begun, claim hackers," *The Observer*, http://www.guardian.co.uk/media/2010/dec/11/wikileaks-backlash-cyber-

war?utm_source=twitterfeed&utm_medium=twitter&utm_campaign=nettechnews (accessed December 11, 2010).

[19] Robert Coalson, "Behind The Estonia Cyberattacks," *Radio Free Europe / Radio Liberty - Free Media in Unfree Societies*, http://www.rferl.org/content/Behind_The_Estonia_Cyberattacks/1505613.html (accessed December 4, 2010).

[20] Liang Qiao, Al Santoli, and Wang Xiangsui. *Unrestricted warfare: China's master Plan to Destroy America* (News Max Media, Inc., 2002), Google e-book.

[21] Ibid.

[22] James Turitto, "Understanding Warfare in the 21st Century," *International Affairs Review*, Volume XVIII No 3: Winter 2010, (accessed September 20, 2010).

[23] William Caldwell, "Changing the Organizational Culture (Updated) (SWJ Blog)," *Small Wars Journal*. http://smallwarsjournal.com/blog/2008/02/changing-the-organizational-cu-1/ (accessed February 3, 2011).

[24] John Markoff and David Barboza, "Two Chinese Schools Said to Be Tied to Online Attacks," *The New York Times*, http://query.nytimes.com/gst/fullpage.html?res=9C02E5DD1131F93AA25751C0A9669D8B63&sec=&spon=&pagewanted=all (accessed December 4, 2010).

[25] Mao Tse-tung, "Dynamics of Revolution: The Army," in *U.S. Army War College Guide to National Security Issues Vol. II: Theory of War and Strategy,* (Carlisle Barracks, PA: U.S. Army War College, 2010), 68.

[26] Austin Long, "COIN Theory: What are Insurgencies and How Does One Fight Them," in *U.S Army War College Guide to National Security Issues Vol. II: Theory of War and Strategy,* 4th ed. (Chapel Hill: U.S. Government, 2010), 147.

[27] Sun Tzu, *The Art of War*, 88.

[28] Barack Obama, *The National Security Strategy of U.S. of America* (Washington D.C.: The White House, May 2010), 10.

[29] Obama, *The National Security Strategy of U.S. of America*, 10.

[30] U.S. Congress, House of Representatives, Committee on Foreign Affairs, *The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security, and Trade*, March 10, 2010, 4.

[31] James C. Mulvenon, "The PLA and Information Warfare" in *The People's Liberation Army in the Information Age* (Santa Monica, CA: Rand Corporation,1999), Google e-book, 183.

[32] Ibid., 176. In his work. Mr. Mulvenon uses the Joint Publication 3-13 to define information warfare as "information operations conducted in time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries."

[33]Ibid.

[34] "U.S. Computer Emergency Readiness Team Makes Progress in Securing Cyberspace, but Challenges Remain," June 7, 2010, linked from *The Department of Homeland Security Home Page,* http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_10-94_Jun10.pdf (accessed November 10, 2010).

[35]William Waddell, "The DoD/DHS Cyber Lash Up: Business as Usual or Government Expansion," linked from *The U.S. Army War College Home Page* at "DIME Blog," http://www.carlisle.army.mil/dime/blog/archivedArticle.cfm?blog=dime&id=141 (accessed February 3, 2011).

[36]Scott Fontain. "Decoding the Secret in Cyber Command Logo," *Marine Corps Times*, July 9, 2010, http://www.marinecorpstimes.com/ news/2010/07/ airforce_cyber_command_logo_070910w/ (accessed October 16, 2010).

[37]Waddell, "The DoD/DHS Cyber Lash Up: Business as Usual or Government Expansion."

[38]Ibid.

[39]Georgia Tech Information Security Center, "Emerging Cyber Threats Report 2011," *Mobile Active Defense*, http://www.mobileactivedefense.com/wp-content/uploads/2010/10/gtisc_report_2010.pdf (accessed November 11, 2010).

[40]According to PCMAG.com's encyclopedia, a "botnet" is a group of computers that have been compromised by a Trojan and are then used to send span or viruses or flood a network as part of a denial of service attack. *PCMag.com*, http://pcmag.com/encyclopedia/.

[41]Elinor Mills, "Study: Cybercrime Cost Firms $1 Trillion Globally," *CNET News*, http://news.cnet.com/8301-1009_3-10152246-83.html (accessed November 11, 2010).

[42]Jim Harper, ". . . But What Is "Cyber"?" *Cato @ Liberty*, http://www.cato-at-liberty.org/but-what-is-cyber/ (accessed November 11, 2010).

[43]Georgia Tech Information Security Center. "Emerging Cyber Threats Report 2011."

[44]Ellen Nakashima, "Pentagon's Cyber Command Seeks Authority to Expand its Battlefield." *The Washington Post,* November 6, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/11/05/AR2010110507304.html (accessed November 6, 2010).

[45]"Michael Schmitt, "Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy," The National Academies Press. http://books.nap.edu/openbook.php?record_id=12997&page=155 (accessed November 12, 2010).

[46]Air Force Major Eric Holdaway provides a good background paper on active and passive defensive measures on networks available in "Active Computer Network Defense: An Assessment" at http://www.iwar.org.uk/iwar/resources/ usaf/Maxwell.students/2001/01-055.pdf.

[47] Michael Schmitt, "Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy."

[48] Sun Tzu, *The Art of War*, 98.

[49] Richard Powers, "Frontline: Hackers: The Risks: The Dangers Confronting Computer Users, Corporations and Governments," interview with *Public Broadcasting Service*, http://www.pbs.org/wgbh/pages/frontline/shows/hackers/risks/dangers.html (accessed February 3, 2011).

[50] Gulio Douhet, "Command of the Air," in *U.S. Army War College Guide to National Security Issues Vol. I: Theory of War and Strategy,* (Carlisle Barracks, PA: U.S. Army War College, 2010), 285.

[51] Sun Tzu, *The Art of War*, 69.

[52] Ibid., 85.

[53] Clausewitz, *On War*, 358.

[54] U.S. Joint Chiefs of Staff, *Homeland Defense,* Joint Publication 3-27 (Washington, D.C.: U.S. Joint Chiefs of Staff, 2007) 1-8.

[55] Stephen Korns and Joshua Kastenberg, "Georgia's Cyber Left Hook," *Parameters* Vol. XXXVIII, no. 4 (Winter 2008-2009). Reproduced on *The U.S. Army Homepage*, http://www.army.mil/-news/2009/04/07/19351-georgias-cyber-left-hook/ (accessed December 8, 2010).

[56] David Smith, "The Fourth Front: Russia's Cyber-attack on Georgia," The Georgian Daily Independent Voice, March 25, 2009, http://georgiandaily.com/ index.php?option=com_content& task=view&id=10757&Itemid=132 (accessed December 8, 2010).

[57] Stephen Korns and Joshua Kastenberg, "Georgia's Cyber Left Hook."

[58] Robert Gates, "Establishment of a Subordinate Under U.S. Strategic Command for Military Cyberspace Operations Unified U.S. Cyber Command," *Wall Street Journal Online*, June 23, 2009, http://www.online.wsj.com/public/resources/documents/ OSD05914.pdf (accessed October 15, 2010).

[59] This perception is based on the author's own experience having been assigned an Information Operations mission while assigned to U.S. Pacific Command in 2009-2010.

[60] William Lynn, "Cybersecurity - Defending a New Domain," linked from *The Official Home of the Department of Defense*, http://www.defense.gov/home/features/ 2010/0410_cybersec/lynn-article1.aspx (accessed October 10, 2010).

[61] Kevin Coleman, "Cyber War 2.0" Russia v. Georgia," *DefenseTech*, August 13, 2008, http://defensetech.org/ 2008/08/13/cyber-war-2-0-russia-v-georgia/ (accessed October 17, 2010).

[62] U.S. Congress, House of Representatives, Committee on Foreign Affairs, *The Google Predicament: Transforming U.S. Cyberspace Policy to Advance Democracy, Security, and Trade*, 4.

[63] Robert McMillan, "Was Stuxnet Built to Attack Iran's Nuclear Program?" PCWorld, September 21, 2010, http://www.pcworld.com/businesscenter/article/205827/was_stuxnet_built_to_attack_irans_nuclear_program.html (accessed October 17, 2010).

[64] Jim Wolf, "U.S. Cyber Command Slips Behind Schedule" *Reuters,* October 1, 2010, http://www.reuters.com/ article/idUSTRE6905AL20101001 (accessed October 17, 2010).